4款常用以太坊智能合约钱包的用户体！到目前为止，大多数在以太坊网络上创建的帐户都属于EOA(外部拥有的帐户)类型，这些帐户受私钥保护。，通常转换成12字(或24字)&quot助记符&quot对于用户来说。如果用户丢失了这些短语，就意味着账户中的资产将永远丢失。

和另一个账户类型——合约账户受代码保护。这提供了便利和各种附加功能，EOA帐户可以&#039；t提供，但它面临的最大威胁是契约代码的安全性。

了解EOA账户和合约账户之间的根本区别非常重要。通过用私钥创建和签署交易，一个EOA账户可以向其他EOA账户或其他合约账户发送消息，而两个EOA账户之间的消息只是简单的值传输。然而，从EOA帐户发送到合约帐户的消息可以激活合约帐户的代码，并允许它执行各种操作(例如转移代币、写入内部存储、发行新硬币、执行计算、创建新合约等)。).

不同于EOA账户，，合同账户可以&#039；不要自己启动新的事务。相反，合约账户只能通过响应其接受的交易来触发自己的交易。

也就是说，以太坊区块链上的当前操作总是由EOA账户触发的交易发起。

而我今天要重点介绍的账户就是后一种类型：合约账户，由此演化出来的一种钱包叫做智能合约钱包。目前主要分为两种：单签名智能合约钱包和多签名智能合约钱包。涉及的钱包有Argent，Authereum，gnosis，MYKEY等等。

体验完这四款钱包，让&#039；让我们简单谈谈它们的异同。

相似性：所有&quot智能合同&quot钱包提供元交易功能。简单来说，就是允许用户通过ERC-20代币支付交易所需的油费(相比之下，EOA钱包只能用ETH支付油费)，这可以大大提高用户体验。此外这些&quot智能合同&quot钱包通过引入一种类似于&quot卫报&quot，在账户丢失的情况下可以省钱。

Let&#039；让我们再来谈谈区别：Argent完全抛弃了记忆术的概念。Gnosis、MYKEY和Authereum仍然提供助记选择。在门槛上，无助记符的Argent钱包显然是最低的，而其他提供助记符选择的智能合约钱包则提供了一种替代的恢复选择。

让&#039；下面我们来说说每个钱包的具体经历和感受：

1。Argent

Argent今年获得由范式基金领投的1200万美元A轮融资。,co-founderRobertLesner,SiliconValleyInvestmentInstitutionIndexVentureCapitalCompanyandFirstMinuteCapitalParticipation

可注册ENS域名作为账户身份，便于识别和管理。您需要提供您的手机号码和电子邮件地址(相当于KYC，用于接收可疑活动报警)，然后设置您的密码和指纹(可选)。全程不需要记录助记符。

添加&quot卫报&quot，您可以选择其他Argent帐户(合约帐户)或EOA帐户，如hardwarewallet和MetaMask。

Atpresent,thechallengeapplicationssupportedbyArgentincludeAave,Compound,kyber,pooltogether,Uniswap,Daidepositinterestrateandsoon

.

APP设置了每日限额调整功能，默认设置为10ETH。用户可以自行调整，但是太高过不去，为了防止Guardian一次性盗取所有资产。

删除APP重新下载后，可以直接导入之前注册的账号，无需找回，带来便利的同时也可能带来一些安全隐患。新手机上的

由&quot找到你的钱包&quot和&quot卫报&quot，你可以让他们锁或者帮你找回钱包。

交易手续费可能比一般EOA账户高；

2.ThebetaversionofAuthereumwallet

hasbeenawardedtheBitcoinbase?Venturecapital,1confirmation,SynapseCapitalandotherinstitutionsinvested1.1millionUSdollars.

你不&#039；t不需要下载app，可以自由设置用户名，需要输入邮箱，然后设置密码；

设置恢复账户，输入对应地址(需要掌握该地址的私钥或助记符)；

可以设置2FA

再次登录时，输入用户名或邮箱和密码即可登录对应的钱包；

忘记密码可以通过还原账号或助记符重置；

2月，白帽黑客samczsun发现了一个致命漏洞，使得攻击者可以控制所有用户&#039；资金。后来团队很快解决了问题，避免了用户的损失。

3、诊断安全

Gnosis在2017年的代币融资潮中获得25万ETH融资。

注册仍然需要助记符(12个英文单词)，没有填写手机号和邮箱的过程；

多签同时支持EOA账户和合约账户，支持2FA功能，相当于加了一把保护锁；

需要一笔安全创建费(随网络情况浮动，撰写本文时为0.01518ETH，约3美元)，门槛相对较高；

对于恢复，备份不一定是你的家人或朋友。它们也可以是硬件钱包设备或您可以访问的其他帐户。

根据创始人的说法，Gnosis正在做的另一个替代恢复选项是基于时间条件的，这简单地意味着允许用户为钱包设置一个规则。如果一年内没有交易，另一个指定账户可以触发订单，收回资金。

4。MYKEY[XY002][XY001]KEY集团，MYKEY所属的公司，去年完成了数千万元的A轮融资。本轮融资由HashKeyCapital领投，分布式资本、复星集团联合创始人梁信军、金融科技投资机构UVA参与投资。

注册后，您仍然需要记住&quot管理私钥&quot(12个助记符，中文默认，英文可选)。&quot管理私钥&quot拥有账户的最高权限，可以冻结和修改其他&quot操作私钥&quot并替换&quot管理私钥&quot本身。

没有填写手机号和邮箱的过程；

根据白皮书中的描述，一个账号的紧急联系人最多可以设置为6个，但目前APP中实际的紧急联系人默认为MYKEYLab，并不是独立设置的。需要等待21天。

如果用户丢失了设备和管理私钥，紧急帮助者可以帮助找回私钥。

除了支持ETH，还支持EOS。

开户需要几分钟，开户后会给你官方0.5美元(keytoken)作为交易费。

对了，除了以上四款智能合约钱包，市场上也有基于第二层的智能合约钱包(如ZK-Rollup)。这种智能合约钱包可以实现超低手续费，扩展以太坊，其他功能与上述智能合约钱包类似。

需要明确指出的是，以上智能合约钱包都是基于社会回收的。但是使用社会恢复实际上会带来人为因素，通常会引入漏洞，不仅涉及合谋风险，还会引入其他攻击可能性，所以设置合理的挑战期并提供异常通知功能是非常必要的。

另外还有EIP2429等方案，可以实现&quot信任最小化&quot，但是到现在为止，我不&#039；Idon’ 我似乎还没有发现一个具有类似方案的智能合约钱包。

最后说点不负责任的话：

智能合约钱包将是大势所趋，但相关的钱包其实还处于非常初级的阶段。他们的安全性需要时间来证明(谁知道什么时候会暴露一个致命的漏洞)；

短期内仍是EOA钱包的天下。比如作者还是会选择使用助记符；

以太坊主网就是这么堵的。不是&#039；基于第二层转移钱包香不香？所以个人会期待基于Rollup的智能合约钱包；

高门槛有利于安全，低门槛有利于采用。怎么平衡真的有点头疼。在我体验过的几款智能合约钱包中，只有Gnosis是收费的；